http://didawiki.di.unipi.it/doku.php/magistraleinformatica/psc/

PSC 2020/21 (375AA, 9CFU)

Principles for Software Composition

Roberto Bruni
http://www.di.unipi.it/~bruni/

Exercises #5

HOFL, type inference and operational semantics

[Ex. 1] Determine the type of the HOFL term

$$t \stackrel{\text{def}}{=} \mathbf{rec}\ x.\ ((\lambda y.\ \mathbf{if}\ y\ \mathbf{then}\ 0\ \mathbf{else}\ 0)\ x).$$

Then compute its (lazy) canonical form.

Ex. 1, typing

$$t \triangleq \underbrace{\mathbf{rec}\ \underbrace{x}_{int}.\ \underbrace{(\ \underbrace{(\ \lambda \underbrace{y}_{int}.\ \underbrace{\mathbf{if}\ \underbrace{y}_{int}\ \mathbf{then}\ \underbrace{0}_{int}\ \mathbf{else}\ \underbrace{0}_{int}}_{int}\ )}_{int \to int}\ \underbrace{x}_{int}\ )}_{int}}_{int} \quad : int$$

Ex. 1, canonical form?

$$t \triangleq \textbf{rec}\ x.\ (\ (\ \lambda y.\ \textbf{if}\ y\ \textbf{then}\ 0\ \textbf{else}\ 0\ )\ x\ ) \quad : int$$

$$t \to c \ \nwarrow\ (\ (\ \lambda y.\ \textbf{if}\ y\ \textbf{then}\ 0\ \textbf{else}\ 0\ )\ x\ )[{}^{t}/_{x}] \to c$$

$$= (\ (\ \lambda y.\ \textbf{if}\ y\ \textbf{then}\ 0\ \textbf{else}\ 0\ )\ t\ ) \to c$$

$$\nwarrow\ \lambda y.\ \textbf{if}\ y\ \textbf{then}\ 0\ \textbf{else}\ 0 \to \lambda x'.\ t'\ ,\ t'[{}^{t}/_{x'}] \to c$$

$$\nwarrow_{x'=y, t'=\textbf{if}\dots}\ (\ \textbf{if}\ y\ \textbf{then}\ 0\ \textbf{else}\ 0\ )[{}^{t}/_{y}] \to c$$

$$= (\ \textbf{if}\ t\ \textbf{then}\ 0\ \textbf{else}\ 0\ ) \to c$$

$\nwarrow\ t \to n,\ 0 \to c$ (it doesn't matter if $n = 0$)

same goal from which we started:
no canonical form

[**Ex. 2**] Determine the type of the HOFL term

$$map \stackrel{\text{def}}{=} \lambda f.\ \lambda x.\ ((f\ \mathbf{fst}(x)), (f\ \mathbf{snd}(x)))$$

Then, compute the (lazy) canonical forms of the terms

$$t_1 \stackrel{\text{def}}{=} map\ (\lambda z.\ 2 \times z)\ (1,2) \qquad\qquad t_2 \stackrel{\text{def}}{=} \mathbf{fst}\ (\ map\ (\lambda z.\ 2 \times z)\ (1,2)\ )$$

Ex. 2, typing

$$map \triangleq \lambda f \;.\; \lambda x \;.\; (\; (\; f \;\; \mathbf{fst}(x) \;) \;,\; (\; f \;\; \mathbf{snd}(x) \;) \;)$$

$f : \tau_1 \to \tau$, $x : \tau_1 * \tau_1$

$f : \tau_1 \to \tau$, $x : \tau_1 * \tau_2$, $f : \tau_1 \to \tau$, $x : \tau_1 * \tau_2$

$\mathbf{fst}(x) : \tau_1$, $\mathbf{snd}(x) : \tau_2 = \tau_1$

$(f \;\mathbf{fst}(x)) : \tau$, $(f \;\mathbf{snd}(x)) : \tau$

$((f \;\mathbf{fst}(x)), (f \;\mathbf{snd}(x))) : \tau * \tau$

$\lambda x \;.\; \ldots : \tau_1 * \tau_1 \to \tau * \tau$

$\lambda f \;.\; \lambda x \;.\; \ldots : (\tau_1 \to \tau) \to \tau_1 * \tau_1 \to \tau * \tau$

$$map \;:\; (\tau_1 \to \tau) \to \tau_1 * \tau_1 \to \tau * \tau$$

Ex. 2a, canonical form

$$map \triangleq \lambda f\ .\ \lambda x\ .\ (\ (\ f\ \mathbf{fst}(x)\ )\ ,\ (\ f\ \mathbf{snd}(x)\ )\ )$$

$$t_1 \triangleq map\ (\lambda z.\ 2 \times z)\ (1,2)$$

$$t_1 \to c\ \nwarrow\ \ (map\ (\lambda z.\ 2 \times z)) \to \lambda x'.\ t'\ ,\ t'[^{(1,2)}/_{x'}] \to c$$

$$\nwarrow\ map \to \lambda f'.\ t''\ ,\ t''[^{\lambda z.\ 2\times z}/_{f'}] \to \lambda x'.\ t'\ ,\ t'[^{(1,2)}/_{x'}] \to c$$

$$\nwarrow_{f'=f,t''=\lambda x\ldots}\ (\lambda x.\ ((f\ \mathbf{fst}(x)),(f\ \mathbf{snd}(x))))[^{\lambda z.\ 2\times z}/_{f}] \to \lambda x'.\ t'\ ,\ t'[^{(1,2)}/_{x'}] \to c$$

$$= (\lambda x.\ (((\lambda z.\ 2 \times z)\ \mathbf{fst}(x)),((\lambda z.\ 2 \times z)\ \mathbf{snd}(x)))) \to \lambda x'.\ t'\ ,\ t'[^{(1,2)}/_{x'}] \to c$$

$$\nwarrow_{x'=x,t'=(\ldots,\ldots)}\ (((\lambda z.\ 2 \times z)\ \mathbf{fst}(x)),((\lambda z.\ 2 \times z)\ \mathbf{snd}(x)))[^{(1,2)}/_{x}] \to c$$

$$= (((\lambda z.\ 2 \times z)\ \mathbf{fst}(1,2)),((\lambda z.\ 2 \times z)\ \mathbf{snd}(1,2))) \to c$$

$$\nwarrow_{c=(((\lambda z.\ 2\times z)\ \mathbf{fst}(1,2)),((\lambda z.\ 2\times z)\ \mathbf{snd}(1,2)))}\ \square$$

Ex. 2b, canonical form

$$t_1 \to (\ ((\lambda z.\ 2 \times z)\ \mathbf{fst}(1,2))\ ,\ ((\lambda z.\ 2 \times z)\ \mathbf{snd}(1,2))\ )$$

$$\mathbf{fst}(t_1) \to c \ \nwarrow\ \ t_1 \to (t'_1, t'_2)\ ,\ t'_1 \to c$$

$$\nwarrow^{*}_{t'_1=(\lambda z.\ 2\times z)\ \mathbf{fst}(1,2)\ ,\ t'_2=(\lambda z.\ 2\times z)\ \mathbf{snd}(1,2)} (\lambda z.\ 2 \times z)\ \mathbf{fst}(1,2) \to c$$

$$\nwarrow\ \lambda z.\ 2 \times z \to \lambda z'.\ t'\ ,\ t'[^{\mathbf{fst}(1,2)}/_{z'}] \to c$$

$$\nwarrow_{z'=z, t'=2\times z}\ (2 \times z)[^{\mathbf{fst}(1,2)}/_{z}] \to c$$

$$= (2 \times \mathbf{fst}(1,2)) \to c$$

$$\nwarrow_{c=n_1 \underline{\times} n_2}\ 2 \to n_1\ ,\ \mathbf{fst}(1,2) \to n_2$$

$$\nwarrow^{*}_{n_1=2}\ (1,2) \to (t''_1, t''_2)\ ,\ t''_1 \to n_2$$

$$\nwarrow_{t''_1=1, t''_2=2}\ 1 \to n_2$$

$$\nwarrow_{n_2=1}\ \square$$

$$c = n_1 \underline{\times} n_2 = 2 \underline{\times} 1 = 2$$

Domain theory

[**Ex. 3**] Let $(D, \sqsubseteq_D)$ be a CPO and $f : D \to D$ be a continuous function. Prove that the set of fixpoints of f is itself a CPO (ordered by $\sqsubseteq_D$).

Ex. 3, CPO of fixpoints

$(D, \sqsubseteq_D)$ CPO $\qquad f : D \to D$ continuous

$\mathsf{FP}_f \triangleq \{ \; d \;\mid\; d = f(d) \; \}$ set of all fixpoints of f

$(\mathsf{FP}_f, \sqsubseteq) \qquad \sqsubseteq \triangleq \sqsubseteq_D \cap (\mathsf{FP}_f \times \mathsf{FP}_f)$ CPO?

it is a PO (because $\mathsf{FP}_f \subseteq D$)

we prove it is complete take a chain $\{d_i\}_{i\in\mathbb{N}} \subseteq \mathsf{FP}_f$

we show that $\bigsqcup_{i\in\mathbb{N}} d_i$ as computed in D is a fixpoint of f

$$f\left(\bigsqcup_{i\in\mathbb{N}} d_i\right) = \bigsqcup_{i\in\mathbb{N}} f(d_i) \qquad \text{by continuity}$$

$$= \bigsqcup_{i\in\mathbb{N}} d_i \qquad \text{each } d_i \text{ is a fixpoint}$$

HOFL denotational semantics

[Ex. 4] (Test for convergence) We would like to modify the denotational semantics of HOFL assigning to the construct

$$\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1$$

- the semantics of t_1 if the semantics of t is $\perp_{\mathbb{Z}_\perp}$, and
- the semantics of t_0 otherwise.

Is it possible? If not, why?

Ex. 4, convergence test

$$[\![\mathbf{if}\ t\ \mathbf{then}\ t_0\ \mathbf{else}\ t_1]\!]\rho \triangleq \mathsf{Cond}_\tau^\perp(\ [\![t]\!]\rho\ ,\ [\![t_0]\!]\rho\ ,\ [\![t_1]\!]\rho\ )$$

$$\mathsf{Cond}_\tau^\perp(v, d_0, d_1) \triangleq \begin{cases} d_0 & \text{if } v = \lfloor n \rfloor \text{ for some } n \\ d_1 & \text{otherwise} \end{cases}$$

Any problem?

$\mathsf{Cond}_\tau^\perp$ is not monotone on *v* !

Counterexample $\perp_{\mathbb{Z}_\perp} \sqsubseteq_{\mathbb{Z}_\perp} \lfloor 1 \rfloor$ Take $d_1 \not\sqsubseteq_{D_\tau} d_0$

$$(\perp_{\mathbb{Z}_\perp}, d_0, d_1) \sqsubseteq_{\mathbb{Z}_\perp \times D_\tau \times D_\tau} (\lfloor 1 \rfloor, d_0, d_1)$$

$$\mathsf{Cond}_\tau^\perp(\perp_{\mathbb{Z}_\perp}, d_0, d_1) = d_1 \not\sqsubseteq_{D_\tau} d_0 = \mathsf{Cond}_\tau^\perp(\lfloor 1 \rfloor, d_0, d_1)$$

Ex. 4, convergence test

For example take $d_0 = \lfloor 0 \rfloor \qquad d_1 = \lfloor 1 \rfloor$

$$[\![\textbf{if rec } x.\ x \textbf{ then } 0 \textbf{ else } 1]\!]\rho = \lfloor 1 \rfloor$$
$$\not\sqsubseteq_{\mathbb{Z}_\bot}$$
$$[\![\textbf{if } 1 \textbf{ then } 0 \textbf{ else } 1]\!]\rho = \lfloor 0 \rfloor$$

as a consequence

$$t \triangleq \lambda x.\ \textbf{if } x \textbf{ then } 0 \textbf{ else } 1 \ : \ int \to int$$

has no possible semantics in $D_{int \to int} = [\mathbb{Z}_\bot \to \mathbb{Z}_\bot]_\bot$

because $[\![t]\!]\rho$ is not continuous (not monotone)

[**Ex. 5**] (Strict conditional) Modify the operational semantics of HOFL by taking the following rules for conditionals:

$$\frac{t \to 0 \quad t_0 \to c_0 \quad t_1 \to c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \;\to\; c_0} \qquad \frac{t \to n \quad n \neq 0 \quad t_0 \to c_0 \quad t_1 \to c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \;\to\; c_1}.$$

Without changing the denotational semantics, prove that:

1. for any term t and canonical form c, we have $t \to c \;\Rightarrow\; \forall \rho.\; [\![t]\!]\,\rho = [\![c]\!]\,\rho$;
2. in general $t\Downarrow \not\Rightarrow t\downarrow$ (exhibit a counterexample).

Ex. 5.1, correctness

$$\frac{t \rightarrow 0 \quad t_0 \rightarrow c_0 \quad t_1 \rightarrow c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \;\; \rightarrow \;\; c_0} \qquad \frac{t \rightarrow n \quad n \neq 0 \quad t_0 \rightarrow c_0 \;\; t_1 \rightarrow c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \;\; \rightarrow \;\; c_1}.$$

$$t \rightarrow c \;\Rightarrow\; \forall \rho.\ \llbracket t \rrbracket\, \rho = \llbracket c \rrbracket\, \rho$$

$$P(t \rightarrow c) \triangleq \forall \rho.\ \llbracket t \rrbracket \rho = \llbracket c \rrbracket \rho$$

we extend the proof of correctness (by rule induction)
to consider the new rules

Ex. 5.1, correctness

$$P(t \to c) \triangleq \forall \rho.\ [\![t]\!]\rho = [\![c]\!]\rho$$

$$\frac{t \to 0 \quad t_0 \to c_0 \quad t_1 \to c_1}{\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \ \to\ c_0}$$

assume

$$P(t \to 0) \triangleq \forall \rho.\ [\![t]\!]\rho = [\![0]\!]\rho = \lfloor 0 \rfloor$$

$$P(t_0 \to c_0) \triangleq \forall \rho.\ [\![t_0]\!]\rho = [\![c_0]\!]\rho$$

$$P(t_1 \to c_1) \triangleq \forall \rho.\ [\![t_1]\!]\rho = [\![c_1]\!]\rho$$

we want to prove

$$P(\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1 \to c_0) \triangleq \forall \rho.\ [\![\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1]\!]\rho = [\![c_0]\!]\rho$$

$$\begin{aligned}
[\![\textbf{if } t \textbf{ then } t_0 \textbf{ else } t_1]\!]\rho &= \mathsf{Cond}_\tau([\![t]\!]\rho, [\![t_0]\!]\rho, [\![t_1]\!]\rho) && \text{by def} \\
&= \mathsf{Cond}_\tau(\lfloor 0 \rfloor, [\![c_0]\!]\rho, [\![c_1]\!]\rho) && \text{by ind. hyp.} \\
&= [\![c_0]\!]\rho && \text{by Cond}
\end{aligned}$$

Ex. 5.1, correctness

$$P(t \to c) \triangleq \forall \rho.\ [\![t]\!]\rho = [\![c]\!]\rho$$

$$\frac{t \to n \quad n \neq 0 \quad t_0 \to c_0 \quad t_1 \to c_1}{\textbf{if}\ t\ \textbf{then}\ t_0\ \textbf{else}\ t_1 \ \to\ c_1}$$

assume $P(t \to n) \triangleq \forall \rho.\ [\![t]\!]\rho = [\![n]\!]\rho = \lfloor n \rfloor \quad n \neq 0$

$P(t_0 \to c_0) \triangleq \forall \rho.\ [\![t_0]\!]\rho = [\![c_0]\!]\rho$

$P(t_1 \to c_1) \triangleq \forall \rho.\ [\![t_1]\!]\rho = [\![c_1]\!]\rho$

we want to prove

$$P(\textbf{if}\ t\ \textbf{then}\ t_0\ \textbf{else}\ t_1 \to c_1) \triangleq \forall \rho.\ [\![\textbf{if}\ t\ \textbf{then}\ t_0\ \textbf{else}\ t_1]\!]\rho = [\![c_1]\!]\rho$$

$[\![\textbf{if}\ t\ \textbf{then}\ t_0\ \textbf{else}\ t_1]\!]\rho = \mathsf{Cond}_\tau([\![t]\!]\rho, [\![t_0]\!]\rho, [\![t_1]\!]\rho)$ by def

$= \mathsf{Cond}_\tau(\lfloor n \rfloor, [\![c_0]\!]\rho, [\![c_1]\!]\rho)$ by ind. h.

$= [\![c_1]\!]\rho$ by Cond

Ex. 5.2, inconsistency

we want to find a term t such that $t \Downarrow$ $\quad$ $t \uparrow$

take $\quad t \triangleq \textbf{if } 0 \textbf{ then } 1 \textbf{ else rec } x.\ x \ :\ int$

$$[\![t]\!]\rho = \mathsf{Cond}_{int}([\![0]\!]\rho, [\![1]\!]\rho, [\![\textbf{rec } x.\ x]\!]\rho)$$

$$= \mathsf{Cond}_{int}(\lfloor 0 \rfloor, \lfloor 1 \rfloor, \bot_{\mathbb{Z}_\bot}) \quad = \lfloor 1 \rfloor \qquad t \Downarrow$$

$$t \to c \ \nwarrow \ 0 \to 0\ ,\ 1 \to c\ ,\ \textbf{rec } x.\ x \to c_1$$

$$\nwarrow^{*}_{c=1} \ \textbf{rec } x.\ x \to c_1$$

$$\nwarrow \ x[^{\textbf{rec } x.\ x}/_x] \to c_1$$

$$= \textbf{rec } x.\ x \to c_1 \qquad t \uparrow$$

[**Ex. 6**] Determine the type of the HOFL term

$$t \stackrel{\text{def}}{=} \mathbf{rec}\ f.\ (\ \lambda x.1\ ,\ \mathbf{fst}(f)\ 0\ )$$

Then, compute the (lazy) denotational semantics of t.

Ex. 6, typing

$$t \triangleq \mathbf{rec}\ \underbrace{f}_{(int \to \tau_1) * \tau_2}.\ \underbrace{\underbrace{(\ \lambda \underbrace{x}_{\tau}.\ \underbrace{1}_{int}}_{\tau \to int}\ ,\ \underbrace{(\underbrace{\mathbf{fst}(\ \underbrace{f}_{(int \to \tau_1) * \tau_2}\ )}_{int \to \tau_1}\ \underbrace{0}_{int}\ )}_{\tau_1}\ )}_{(\tau \to int) * \tau_1} \quad : (int \to int) * int$$

$$(int \to \tau_1) * \tau_2 = (\tau \to int) * \tau_1$$

$$\begin{cases} int = \tau \\ \tau_1 = int \\ \tau_2 = \tau_1 \end{cases}$$

$$\tau = \tau_1 = \tau_2 = int$$

Ex. 6, den semantics

$$t \triangleq \mathbf{rec}\ f.\ (\ \lambda x.\ 1\ ,\ (\mathbf{fst}(\ f\ )\ 0\ )\ )\quad : (int \to int) * int$$

$$[\![t]\!]\rho = \mathit{fix}\ \lambda d_f.\ [\![(\lambda x.\ 1, \mathbf{fst}(f)\ 0)]\!]\rho[{}^{d_f}/_f]$$

$$= \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ [\![\lambda x.\ 1]\!]\rho[{}^{d_f}/_f]\ ,\ [\![\mathbf{fst}(f)\ 0]\!]\rho[{}^{d_f}/_f]\ )\ \rfloor$$

$$\rho' = \rho[{}^{d_f}/_f]$$

$$= \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ [\![1]\!]\rho'[{}^{d_x}/_x]\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow [\![\mathbf{fst}(f)]\!]\rho'.\ \varphi([\![0]\!]\rho'))\ )\ \rfloor$$

$$= \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*([\![f]\!]\rho').\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$= \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ d_f.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

Ex. 6, den semantics

$$[\![t]\!]\rho = \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ d_f.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$f_0 = \bot_{D_{(int \to int) * int}}$$

$$f_1 = \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ f_0.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$= \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ \bot_{D_{int}}\ )\ \rfloor$$

$$f_2 = \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ f_1.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$= \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$= \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\lambda d_x.\ \lfloor 1 \rfloor)\ \lfloor 0 \rfloor\ )\ \rfloor$$

$$= \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ \lfloor 1 \rfloor\ )\ \rfloor$$ maximal element!

Ex. 6, den semantics

$$t \triangleq \mathbf{rec}\ f.\ (\ \lambda x.\ 1\ ,\ (\mathbf{fst}(\ f\ )\ 0\ )\ )\quad : (int \to int) * int$$

$$[\![t]\!]\rho = \mathit{fix}\ \lambda d_f.\ \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ (\mathbf{let}\ \varphi \Leftarrow \pi_1^*\ d_f.\ \varphi\ \lfloor 0 \rfloor)\ )\ \rfloor$$

$$[\![t]\!]\rho = \lfloor\ (\ \lfloor\ \lambda d_x.\ \lfloor 1 \rfloor\ \rfloor\ ,\ \lfloor 1 \rfloor\ )\ \rfloor$$